(12) UK Patent Application (19) GB (11) 2 322 035 (13) A

(43) Date of A Publication 12.08.1998

(21) Application No 9702355.0

(22) Date of Filing 05.02.1997

(71) Applicant(s)
Stuart Justin Nash
22 Hills Road, CAMBRIDGE, CB2 1JP, United Kingdom

(72) Inventor(s)
Stuart Justin Nash

(74) Agent and/or Address for Service
Keith W Nash & Co
90-92 Regent Street, CAMBRIDGE, CB2 1DP,
United Kingdom

(51) INT CL[6]
H04M 11/06 , G06F 1/00

(52) UK CL (Edition P)
H4K KOD4 KOD6
G4A AAP

(56) Documents Cited
GB 2306079 A GB 2229020 A EP 0067611 A1
WO 88/07240 A1 WO 86/03864 A1 US 4779224 A
US 4685124 A

(58) Field of Search
UK CL (Edition O) G4A AAP , H4K KOD4 KOD5 KOD6
INT CL[6] G06F 1/00 , H04M 11/06
ONLINE: WPI

(54) Abstract Title
Computer connected to telecommunication network modem via buffer computer

(57) A computer connected to a telecommunication network via a modem is isolated from the network by a second computer, which acts as a buffer for the receipt and transmission of data and prevents unauthorised access. The second computer may include two drives either on the same hard disc or on separate hard discs. One drive serves as a buffer store for outgoing messages and the other for data received from the telecommunications network. A software or hardware interlock may be provided to prevent simultaneous connection of the two drives to a common computer bus. The second computer may be constructed from one or more expansion cards, fitted inside the first computer. The second computer is such that no connection is provided between the first computer and modem except through an inlet/outlet port on the expansion card and no direct path can be established on the expansion card between the modem inlet/outlet port and the main computer bus. The arrangement is useful with e-mail and communications on the Internet and may use security mechanisms including passwords, virus checks and caller identification.

GB 2 322 035 A

The claims were filed later than the filing date within the period prescribed by Rule 25(1) of the Patents Rules 1995

7/28/2005, EAST Version: 2.0.1.41

2322035

C260.00/N

Title: Improvements in and relating to computers

Field of invention

This invention concerns computers and in particular the connection of computers to telecommunication networks and concerns a device which enables a computer to be isolated from a telecommunications network to avoid direct access thereto by unauthorised outsiders whilst still enabling data transmission or so-called e-mail via the tecommunication network and the Internet.

Background to the invention

It is known to communicate between two computers using a telecommunication network by connecting each of the computers to the telecommunication network via a modem. Whilst one modem is transmitting the other acts as a receiver and vice versa.

Interconnection of computers in this way has enabled national and international communication using the existing telecommunication highways and the Internet as it is now called has become an established communication highway for transmitting and receiving data one particular form of which is so-called e-mail.

In this connection e-mail is identified as letter-like communications or messages made up of words and ordinary numerals which for transmission purposes are coded using the so-called ASCII code and which can be translated by decoding the ASCII code on receipt.

Where a computer is connected permanently to a telephone line via a modem, it has always been possible for a third party to gain access to the computer via the modem if the telephone

number allocated to that line was known by the third party. Having established contact via the modem, it is not impossible to transmit data other than so-called e-mail and computer programmes, executable files, can be transmitted via a modem just as easily as the ASCII code relating to e-mail. Using the system in reverse, a third party gaining access via a modem may choose to inspect records stored on the hard disc of the computer which has been accessed. Both techniques are available for legitimate use but can also be used by third parties for unauthorised purposes.

Various attempts have been made to reduce the risk of virus or other executable file transmission onto a computer, and likewise various techniques and devices have been incorporated including code words, pass words and the like to prevent access to computer records by third parties who are unauthorised to read the contents of the discs.

With the advent of e-mail the problem of security particularly preventing access to sensitive data and preventing the downloading of executable files which might otherwise overcome security techniques already incorporated or destroy data, has become very real.

It is an object of the present invention to provide a simple technique for isolating a computer from the telecommunications network and provide a greater degree of security and minimise the risk of unauthorised access and unauthorised downloading of executable files or other programmes.

Summary of the invention

According to the present invention where a first computer is to be connected to a telecommunication network via amodem, a second computer is provided between the first computer and the modem, the sole purpose of which is to serve as a buffer for the receipt and transmission of data between the first computer

and the telecommunication network.

The second computer preferably includes two drives which may be on the same hard disc or on separate hard discs, onto which data can be written and from which data can be read, the first drive serving as a buffer store for messages which are transmitted from the first computer and are to be transmitted via the modem to the telecommunication network, and the second drive serving as a buffer store for data received from the telecommunication network and which is to be transmitted to the said first computer.

According to a preferred feature of the invention, a software or hardware or combination of software and hardware interlock is provided which prevents simultaneous connection of the two drives to the common computer bus.

According to another preferred feature the said second computer includes two operating programmes one on the first drive, and the other on the second drive and the computer can only be operated so as to run the one programme or the other programme, but not both. By arranging that the one programme only allows access to the one drive and the other programme only access to the other drive, so the computer can only see one or the other of the two drives at any one instant in time.

More preferably a hardware interlock or so-called dongle may be provided and the security of the overall system further improved by providing that the dongle must be in place and one or more pass words entered before either one or both of the different operating programmes can be run. In this way the second computer can be prevented from transmitting data without a first level of authority and possibly a first dongle and more importantly can only be rendered capable of receiving data from the telecommunication network upon the entry of a second password and possibly the fitting of a second dongle either in addition to or instead of the first dongle and more importantly

still, a third level of security is provided which inhibits the transfer of data received by the computer and stored on one of the drives from the second computer to the first computer without the entry of a third pass word and the insertion of a third dongle either in addition to or instead of one or both of the first and second dongles.

According to a further preferred aspect of the invention, a checking routine is provided as a further operating programme within the said second computer which can be called up to read each of the files received by the computer and stored on the data receiving drive to determine the nature of each file and its contents and to identify it as a fully recognisable and safe data file such as would correspond to a simple letter or message characteristic of e-mail, or identify it as an executable file and something which should not be transferred to this first computer without an IT specialist or technologist checking to ensure that the executable file is one which is permitted to be loaded on to the first machine or to check whether the executable file is a so-called virus by comparing the appropriate identification of the virus file with the known virus identification using a readily available virus checking programme.

The checking programme thus filters all files received by the second computer and stored in its appropriate drive into three categories, a first category which are "safe" to be released to the first computer, a second category which may be "safe" to release but may not be desirable to be loaded on the first machine since they might thereafter give a third party access to information or access to the computer which would not normally exist and a third category which are identified as unknown or known viruses and must not, under any circumstances, be downloaded onto the first computer.

According to a further aspect of the invention a further level of security checking is possible by identifying a security code

if it exists a the beginning of any file which falls under the heading of the first or second category and only releasing that document into the first computer if it is appropriate for that file to be downloaded. Thus for example, sensitive incoming messages or programmes which should not have general access can be identified and only downloaded to the first computer in a controlled manner.

The invention thus provides a buffer for intercepting and filtering all incoming e-mail whatever form it takes, and preventing unwanted files from being downloaded onto the computer which may contain data which is sensitive and/or valuable and which is to be protected from unauthorised access or the entry thereon of programmes which could damages or allow unauthorised access to such data.

According to a further preferred feature of the invention, a further interlock is provided which provides an even greater degree of user confidence in ensuring that no external third party can gain unauthorised access to the first computer by providing an interlock such that if a datapath exists between the said second computer and the modem or the modem and the telecommunication network or both, then another datapath between the second computer and the first computer is inhibited or broken and if the datapath between the two computers is established, the datapath between the computer and the modem or the modem and the telecommunications network, must be broken.

The simplest arrangement is a mechanical device or toggle switch such that if the switch is closed to make one path the other path is automatically opened and vice versa.

The interlock may also or instead of be provided by dongles and software entry such as pass words and/or key operation via the keyboard such as dedicated function keys and/or internal programmings which can only be called up uniquely and inhibit

data transfer to or from the computer bus to the appropriate input and output devices. For optimal security, some or all of the different levels and connection and interconnection may be incorporated so that it is virtually impossible to conceive any situation in which all of the interlocks are in place and a data highway can be established between the modem and the output board of the second computer so that data being received from the telecommunication network can pass directly to the said first computer.

In order to improve security for any hardware interlock, this is preferably mounted within a computer and possibly within a sealed element on a computer board which is itself fitted within the computer in such a way that if it is removed or interfered with the computer is immediately disabled in a semi-permanent fashion.

A further level of security can be provided by arranging that a dongle must be present in the second computer such as connected to an output or input port thereof, in manner known per se, and a pass word has been entered before any data can be even recognised by the first computer from the second computer. In this connection further security can be provided by coding and decoding data transmitted between the second computer and the first computer so that only coded data can be read by the first computer and upon decoding will be recognised as valid data by the first computer in addition to the interlock already mentioned so that even if a deliberate attempt is made to bypass the second machine, data from the modem will not be recognised by the first computer since it has not been coded by the second computer as it is stored on the appropriate disc in the second computer or read from that disc before being transmitted to the said first computer.

The invention is of particular application to so-called networks where a large amount of data is stored on one or more servers and a plurality of computers are connected to the

server or servers and data can be shared between various computers forming the network. In such an arrangement one of the computers on the network can be thought of as comprising the said first computer specified above and it is commonplace to connect a telecommunication network thereto by means of a modem to allow e-mail to be transmitted to and from the network so that any user on the network can send and receive e-mail via the external telecommunication network as well as e-mail from any one of the computers connected to its local network. In order to control the traffic, the e-mail either on the local network or for transmission to or from the external telecommunication network is stored on one or more drives on the server and/or one of the nodes of the network so that the receipt and transmission of messages via the telecommunication network does not clash and interference between the two modes of operation is prevented.

In accordance with the present invention, a second computer having the attributes and programmed as previously described is positioned between the modem and the server or node of the network which is normally adapted to communicate with the modem.

The invention thus also lies in a network when modified in this way by the inclusion of an additional computer whose sole purpose is to act as a buffer and isolating device between the member of the network and the external telecommunication network for the receipt and transmission of e-mail.

Although the invention has been described as involving a second computer, the functionality of this additional computer is such that it may be constructed as one or more expansion cards for fitting in the said first computer provided no connection to the first computer is possible by means of a modem except through an inlet/outlet port on the said dedicated board. However in this event it is essential that no direct path can be established on that board between the modem inlet/outlet

port and the computer bus and a fail-safe electromechanical interlock ought to be provided thereon which ensures that the databus on the dedicated board is isolated from the computer databus if a datapath exists between the bus on the dedicated board and the modem and vice versa.

Where a dedicated board is provided, one technique for isolating the modem input from the main computer databus is to provide a first databus on the dedicated board which can only be connected to the modem and a second databus on the dedicated board which can only be connected to the main computer bus and two separate drives and separate processors are provided on the dedicated board, one for receiving data from one bus and transmitting it to the other, and the other for receiving data from the said other bus and transmitting it to the said one bus. By providing a third processor on the dedicated board which can only enable one of the two processors at any one time, and hard coded software on the dedicated board which inhibits the simultaneous operation of the first two processors, so a complete isolation between the two buses is achievable, operation of the board can be achieved using conventional software techniques in the host computer within which the dedicated board is located.

It is to be understood however that the invention is not in any way limited to this arrangement which is merely given by way of example of the many different ways in which the invention can be realised in practice, namely preventing the establishment of a first datapath if a second datapath is already enabled and vice versa.

According to a further aspect of the invention, data which has been received from a telecommunication network and has been stored on one of the drives may be displayed on a computer screen for verification and checking and pass word entry with or without dongles may be required to enable incoming data to be checked and made available for onward transmission to the

first computer.

This aspect of the invention permits a user to check all incoming e-mail and classify the incoming e-mail for security purposes and also check any files which are not recognised as conventional data files to ensure that they are appropriate to be downloaded to the said first computer.

Where a large amount of e-mail is being received and there is no need for security checking and routing of e-mail, the second computer may be programmed so as to check the contents of each file which has been received and is stored on the drive dedicated to incoming mail and to flag each file as it is checked with a pass or fail flag. A simple test is to determine whether the file contains any ASCII code which is outwith the range of codes used for conventional messages involving letters of the alphabet and numerals. Whilst this could exclude scientific texts which entail lesser known characters such as Greek alphabet characters and the like, this would screen out from all of the incoming files all of the e-mail messages which are clearly data files only and leave only those files to be checked which contain questionable ASCII codes.

A further screening can be achieved by running standard virus checker over each file and confirming or denying each flag which has been applied by the first check.

If the e-mail is normally going to comprise scientific texts unusual ASCII codes, a further filter may be provided which can be adapted by entry of appropriate information to permit a cautionary flag to be allocated to the file to indicate that it is essentially a datafile, that it is virus free, but that it contains scientific nomenclature and therefore just needs to be checked from that point of view.

According to a still further aspect of the invention, the

second computer provides a simple mechanism for providing an audit trail for incoming and outgoing e-mail by compiling a database of date, time, telephone number called, duration of call and identity of file so that all messages sent and received can be checked either regularly or as required. With the advent of multiple gigabyte drives in a module which can fit within the normal drive bay of a conventional PC, it is quite possible for two such drives to be provided together with an appropriate programmed computer to serve as the said second computer and to host many thousands of e-mail messages both incoming and outgoing before either of the drives becomes near to capacity.

According to a further aspect of the invention, where automatic checking of each of the incoming files is programmed into the said second computer, a further sub-routine may be provided adapted to generate a warning signal and to introduce a further inhibition on the transfer of data from the second computer to the first computer in the event that any verification process reveals a suspect file. In this way a system operator or other user may be alerted to the fact that a suspect file has been received enabling the operator to take appropriate action as soon as possible after the file has been received and where this turns out to be an attempt by an unauthorised third party to download inappropriate files, the warning may be at such a point in time that the third party may be identified. In order to achieve this, bearing in mind that the third party is using the telecommunication network to route the unwanted data, the invention also envisages the inclusion of the caller identification software in the said second computer and a listing of the telephone number of the calling party to be stored with the data received therefrom, including the date and time of day. In this way, any incoming messages can be identified according to sender so that if data has been received in a scrambled form, the recipient can determine from whom the data was received and advise them accordingly by an appropriate e-mail or telephone call.

C260.00/N

CLAIMS

1. In a system in which a first computer is to be connected to a telecommunication network via a modem, a second computer is provided between the first computer and the modem, the sole purpose of which is to serve as a buffer for the receipt and transmission of data between the first computer and the telecommunication network.

2. A system as claimed in claim 1, wherein the second computer includes two drives which may be on the same hard disc or on separate hard discs, onto which data can be written and from which data can be read, the first drive serving as a buffer store for messages which are transmitted from the first computer and are to be transmitted via the modem to the telecommunication network, and the second drive serving as a buffer store for data received from the telecommunication network and which is to be transmitted to the said first computer.

3. A system as claimed in claims 1 or 2, wherein a software or hardware or combination thereof interlock is provided which prevents simultaneous connection of the two drives to the common computer bus.

4. A system as claimed in any of claims 1 to 3, wherein the second computer includes two operating programmes one on the first drive, and the other on the second drive, and the computer can only be operated so as to run the one programme or the other programme, but not both. By arranging that the one programme only allows access to the one drive and the other programme only access to the other drive, so the computer can only see one or the other of the two drives at any one instant in time.

5. A system as claimed in any of claims 1 to 3, wherein a hardware interlock or so-called dongle is provided and the security of the overall system is further improved by providing that the dongle must be in place and one or more pass words must be entered before either one or both of the different operating programmes can be run, so that the second computer can be prevented from transmitting data without a first level of authority and more importantly can only be rendered capable of receiving data from the telecommunication network upon a second level of authority.

6. A system as claimed in claim 5, wherein the second level of authority is achieved by fitting a second hardware dongle in addition to or in place of the first dongle.

7. A system as claimed in claim 6, wherein a third level of security is provided which inhibits the transfer of data received by the computer and stored on one of the drives from the second computer to the first computer without the entry of a third pass word and the insertion of a third dongle either in addition to or instead of one or both of the first and second dongles.

8. A system as claimed in any of claims 1 to 7, wherein a checking routine is provided as a further operating programme within the said second computer which can be called up to read each of the files received by the computer and stored on the data receiving drive to determine the nature of each file and its contents and to identify it as a fully recognisable and safe data file such as would correspond to a simple letter or message, characteristic of e-mail, or to identify it as an executable file and something which should not be transferred to this first computer before it is checked by one expert to ensure that the executable file is one which can be permitted to be loaded onto the first machine.

9. A system as claimed in claim 8, wherein the check of an identified fie is to determine if the executable file is a so-called virus by comparing the appropriate identification of the virus file with known virus identifications using a readily available virus checking programme.

10. A system as claimed n claim 8 or 9, wherein the checking programme filters all files received by the second computer, and stored in its appropriate drive, into three categories, a first category which are "safe" to be released to the first computer, a second category which may be "safe" to release but may not be desirable to be loaded onto the first machine since they might thereafter give a third party access to information or access to the computer which would not normally exist, and a third category which are identified as unknown or known viruses and must not, under any circumstances, be transferred onto the first computer.

11. A system as claimed in any of claims 5 to 10, wherein a further level of security checking is performed by determining if a security code exists at the beginning of any file which is categorised as falling into the first or second category and only releasing data relating to that document into the first computer if it is appropriate for that file to be downloaded.

12. A buffer for intercepting and filtering all incoming e-mail whatever form it takes, and preventing unwanted files from being downloaded to another computer.

13. A system as claimed in any of claims 1 to 12, wherein a further interlock is provided which provides an even greater degree of user confidence by ensuring that no external third party can gain unauthorised access to the first computer by providing an interlock such that if a datapath exists between the said second computer and the modem, or the modem and the telecommunication network or both, then another datapath between the second computer and the first computer is

interrupted and if the datapath between the two computers is established, the datapath between the computer and the modem or the modem and the telecommunications network, must be interrupted.

14. A system as claimed in claim 13, wherein the interlock is a mechanical device such that if the switch is closed to make one path the other path is automatically opened, and vice versa.

15. A system as claimed in claim 13 or 14, further comprising dongles and software entry such as pass words and/or key operation via the keyboard such as dedicated function keys and/or internal programmings which can only be called up uniquely, to inhibit data transfer to or from the computer bus to the appropriate input and output devices.

16. A system as claimed in any of claims 1 to 15, wherein a hardware interlock is mounted within, optionally within a sealed element on a computer board which is itself fitted within the computer in such a way that if it is removed or interfered with the computer is immediately disabled in a semi-permanent fashion.

17. A system as claimed in any of claims 1 to 16, wherein a further level of security is provided by arranging that a dongle must be present in the second computer such as connected to an output or input port thereof, in manner known per se, and a pass word has to have been entered before any data from the second computer can even be recognised by the first computer.

18. A system as claimed in any of the preceding claims 13 to 17, in which further security is provided by coding and decoding data transmitted between the second computer and the first computer and programming the latter so that only coded data can be read by the first computer, and upon being decoded will be recognised as valid data by the first computer in

addition to the interlock, whereby even if the second machine is bypassed, data from the modem will not be recognised by the first computer since it has not been coded by the second computer.

19. A system as claimed in any of the preceding claims, wherein the second computer, constructed as a single board computer which is adapted to be fitted in an expansion store of the said first computer, and wherein no connection to the first computer is possible by means of a modem except through an inlet/outlet port on the said single computer board.

20. A system as claimed in claim 19, wherein no direct path can be established on the single computer board between the modem inlet/outlet port and the main computer bus, and a fail-safe electromechanical interlock is provided on the board to ensure that the databus on the dedicated board is isolated from the computer databus if a datapath exists between the bus on the dedicated board and the modem and vice versa.

21. A system as claimed in claim 19 or 20, wherein the modem input is isolated from the main computer databus, and a first databus exists on the single computer board which can only be connected to the modem, and a second databus exists on the single board computer which can only be connected to the main computer bus, and two separate drives and separate processors are provided on the single computer board, one for receiving data from one bus and transmitting it to the other, and the other for receiving data from the said other bus and transmitting it to the said one bus.

22. A system as claimed in claim 21, wherein a third processor is provided on the single board computer, which can only enable one of the said two processors at any one time, and hard coded software on the single computer board inhibits the simultaneous operation of the first two processors, whereby complete isolation between the two buses on the single computer board

is achievable.

23. In a system as claimed in any of the preceding claims, data which has been received from a telecommunication network and has been stored on a drive of a first computer is displayable on a computer screen for verification and checking.

24. A system as claimed in claim 23, wherein pass word entry with or without dongles is required to enable incoming data to be checked and made available for onward transmission to the first computer.

25. A system as claimed in any of the preceding claims, wherein the second computer is programmed to provide an audit trail for incoming and outgoing e-mail by compiling a database of date, time, telephone number called, duration of call and identity of file so that all messages sent and received can be checked either regularly or as required.

26. A system as claimed in any of the preceding claims, wherein the caller identification software is incorporated in the said second computer and a listing of the telephone number of a calling party is stored with the data received therefrom, including the date and time of day, whereby each incoming message can be identified according to sender.